Global IT Security

Global IT Security
Edited by Reinhard Posch and György Papp

IT-Security is becoming a baseline technology for the information age. With the emerging infrastructures of cryptography and security systems in general as well as digital signatures IT security is becoming a field of general interest as it concerns a broad public. Covering a broad scope the book focuses on contributions to the following areas:

- Security architecture and security management
- Public key infrastructures and digital signatures
- Access control
- Network security and protocols
- Modelling for security
- Security devices
- Malicious software
- Human factors of security

Global IT Security contains the proceedings of the 14th International Conference on Information Security (SEC '98) sponsored by the International Federation for Information Processing (IFIP), which is held as part of the World Computer Congress (WCC '98) in Vienna and Budapest.
Security appears to be one of the major challenges for the use of information technologies. This situation is widely recognised. The world of communications and transactions is facing a situation where national borders are losing importance and effectiveness. In this context the book will prove to be valuable reading for all interested in IT Security, and should be especially valuable for professionals in networked systems.

Reinhard Posch is head of the department for Applied Information Processing and Communications, Graz University of Technology, Austria. **György Papp** is head of the Department of Informatics and Telecommunication at the Hungarian Prime Minister's office.

Global IT Security

Proceedings of the IFIP TC11 14th international conference on Information Security (SEC '98): 31 August - 2 September 1998, Vienna/AT and Budapest/H

Edited by

György Papp
Prime Minister's office
Hungary

Reinhard Posch
Graz University of Technology
Austria

Published by Austrian Computer Society (OCG) on behalf of the International Federation for Information Processing (IFIP)

Published by Austrian Computer Society, Wollzeile 1-3, 1010 Vienna, Austria
http://www.ocg.or.at

© Österreichische Computer Gesellschaft Komitee für Öffentlichkeitsarbeit

© International Federation for Information Processing (IFIP) 1998

Printed in Austria by Druckerei Riegelnik, A-1080 Wien, Piaristengasse 19

ISBN 3-85403-116-5 Österreichische Computer Ges.

SCHRIFTENREIHE der Österreichischen Computer Gesellschaft BAND 116

Printed by support of Bundesministeriums Für Wissenschaft und Verkehr in Wien

XV. IFIP World Computer Congress
Vienna, Austria / Budapest, Hungary
31 August 1998 – 4 September 1998

CONTENTS

Preface

IFIP SEC'98 Conference Committees

Security and the Internet

1 Security issues surrounding the JavaTM Programming Language
S. Gritzalis, J. Iliadis and V. Oikonomou 3

2 Applet Watch-Dog: A Monitor Controlling the Execution of Java Applets
R. Gorrieri and G. Marchetti 15

3 Robust MPEG Video Copyright Protection Technology
J. Dittmann, M. Stabenau and R. Steinmetz 24

Public Key Infrastructures

4 Key Management
P. Horster, P. Schartner and P. Wohlmacher 37

5 Setting up a Public Certification Authority
P. Lipp, A. Sterbenz and R. Kuch 49

6 Providing X.509-based user access control to web servers
A. Lioy, F. Maino 61

Digital Signatures

7 Efficient Signcryption Schemes On Elliptic Curves
Y Zheng and H. Imai 75

8 An Integrated Approach for Fault Tolerance and Digital Signature in RSA
C. N. Zhang 85

9 A Fast Cryptographic Hash Function Based on Linear Cellular Automata over GF(q)
M. Michaljević, Y. Zheng and H. Imai 96

Network Security

10 Security in TINA
S. Staamann, L. Buttyán and U. Wilhelm 111

11 Design and Implementation of a Secure Distributed Data Repository
A. Iyengar, R. Cahn, C. Jutla and J. A. Garay 123

Access Control

12 Using Ear Biometrics for Passive Identification
M. Burge and W. Burger 139

13 Reference Monitor for Hypermedia-Based Hospital Information Systems
L. J. Janczewski and B. K. W. Lo 149

14 Realization of a Context-Dependent Access Control Mechanism on a Commercial Platform
U. Nitsche, R. Holbein, O. Morger and S. Teufel 160

Protocols

15 Logic-Based Analysis of a New Hybrid Encryption Protocol for Authentication and Key Distribution
M. T. El-Hadidi, N. H. Hegazi and H. K. Aslan 173

16 Tool-Supported Verification of Cryptographic Protocols
C. Eckert 184

17 A New Practical Secure e-Voting Scheme
O. He and Z. Su 196

18 An uncoercible verifiable electronic voting protocol
A. Riera, J. Borrell and J. Rifà 206

Modelling for Security

19 A Role and Task Based Security Model for Multifunctional Smartcard Applications in the Area of Electronic Commerce
K. Schier 219

20 A Purpose-Oriented Access Control Model for Information Flow Management
M. Yasuda, H. Higaki and M. Takizawa 230

21 Can computerized immunity be achieved, based on a biological model?
C. P. Louwrens and S. H. von Solms 240

22 A security model for the design of hypermedia systems
P. Díaz, I. Aedo and A. Ribagorda 251

23 The Application Profile Security Model for Downloaded Executable Content
P. Trommler 261

24 A Group-Enhanced ISSI Model For Secure Interconnection of Information Systems
L. Leiwo and S. Heikkuri 271

Security Architecture

25 Secure Interoperation of Heterogeneous Systems: - A Mediator-Based Approach
S. Dawson, S. Qian, P. Samarati 285

26 An Intelligent Agent Architecture for Securing Internet Trading
X. Yi, E. Okamoto, X. F. Wang and K. Y. Lam 297

27 The Dimensions of Information Security Awareness
M. T Siponen and J. Kajava 309

Security Management

28 Quantitative Evaluation of Information System Security
R. Ortalo and Y. Deswarte 321

29 Concurrency and Synchronisation Issues in Security Implementations
J. P. Bekmann, P. de Goede and A. C. M. Hutchison 333

30 Legal Aspects of Electronic Rights Management Systems (ERMS)
S. Dusollier 344

Security Devices

31 Design flow and modeling for cryptographic macro cells
W. Mayerwieser, K. C. Posch and R. Posch 355

32 Hybrid Random Byte Generators
T. Nemetz and P. Papp 366

Human Factors

33 A Methodology for Comparative Studies of Ethical Opinions related to IT-security issues
L. Yngström 381

34 Competing against human failing
M. E. M. Spruit 392

Malicious Software

35 Reference Audit Information Generation for Intrusion Detection Systems
H. Debar, M. Dacier and A. Wespi 405

36 An Adaptive Intrusion Detection System Using Neural Networks
J. M. Bonifácio Jr, E. S. Moreira, A. M. Cansian and A. C. P. L. F. Carvalho 418

37 Cyber Terrorism
M. J. Warren 429

Policy Update

38 Towards a National and International Policy on Encryption 441
N. Hickson

SHORT PAPER SESSION:

Electronic Commerce

39 A prepaid off-line payment system for electronic money distribution
D. Bruschi and E. Rosti 449

40 Policing the Global Information Infrastructure
S. Pancho 455

41 Detecting violation of real-time constraints in secure electronic commerce transactions
S. Subramanian and M. Singhal 460

Security and the Internet

42 A Model for an European Digital Signature Approach
K. J. Keus and T. Gast 467

43 Secure Conception of Internet Services
P. Kirsch, H. Weidner and K. Bauknecht 477

44 Security Culture in the Global Information Society
A. Hartmann 484

45 Explaining Data Recovery in PGP and Lotus Notes
L. Baranyi 491

Cryptography and Infrastructure

46 The methodology for symmetric encryption algorithms evaluation
M. Stanek and D. Olejar 499

47 A prototype implementation of a system to support multiple certification authorities
H. Chang 504

48 Certificate policies formalisation and evaluation
T. Klobucar and B. Jerman-Blazic 509

49 Breaking the 1 Mbit/s barrier in RSA encryption
J. Großschädl 515

Networks and Modelling

50 Criteria to help develop solutions for securing communications over networks
M. Laurent 523

51 A Model for Access Control and Intrusion Detection in Distributed Systems
G. Mohay 530

52 Predicting development cost of security in distributed software
W. H. Prentner and M. Jazayeri 535

53 A Metric for Trusted Systems
A. Jøsang and S. J. Knapskog 541

Modelling and Management

54 Packaging Information Security Safeguards
R. Baskerville and J. Pries-Heje 549

55 Modelling mix-mediated anonymous communication and preventing pool-mode attacks
E. Franz, A. Graubner, A. Jerichow and A. Pfitzmann 554

56 Telecommunication and Networking Security Activities of the People's Republic of China
E. Kozik 561

57 Security Management Using a Security Related MIB Approach
T.K. Apostolopoulos and K.D. Moulinos 567

Management and Risk

58 An Object Oriented Modelling Approach into the Management of Information Security
J. Leiwo, C. Gamage and Y. Zheng 575

59 Towards an Object Based Access Control model
J.-M. Kabasele-Tenday 580

60 An Intrusion Detection System Based upon Autonomous Mobile Agents
D. Gregory, Q. Shi and M. Merabti 586

61 Modelling risks in a health-care institution
E. Smith and J.H.P. Eloff 592

SPECIAL SESSION:

Developing Steps in Hungarian IT Security

62 Laws, Organisations, Recommendations and Practice
G. Papp, G. Bognár and I. Szabó 601

63 Hungarian IT-Security developments in Banking
J. Brehel 607

64 Education and Research on Security in Hungary
Z. Kincses and Z. Hornák 611

Preface

Introduction by the IFIP President

I take great pleasure to welcome you to the 15th IFIP World Computer Congress on "The Global Information Society on the Way to the Next Millennium".

This Flagship event of the International Federation for Information Processing (IFIP) is a product of the active involvement of hundreds of IT specialists and many national computer societies around the globe. Its programme and agendas are targeted at topical areas of information processing intended to catch your interest and stimulate debate to suit the needs of IT professionals from academia and industry alike.

The debate will aim to disclose the current state-of-the-art and to project the trends for new developments, which will transcend the threshold of the 21st century and lead society in the magic future of technology.

Moreover, the venues of this IFIP Congress are in the heart of Europe. Vienna and Budapest are historical, cultural and technological crossroads of achievement and civilization. These beautiful cities host the IFIP Congress which in turn provides a forum and a platform for people to meet and discuss issues of common interest and concern.

I hope that you will benefit from this exceptional IFIP Event for your daily work and that you have opportunity during the Congress meeting old friends and making many new ones.

Kurt Bauknecht,
University of Zurich,
President of the International Federation for Information Processing - IFIP

Introduction by the Chairman of the International Programme Committee

I am proud to be able to present this technical programme. Out of more than 700 contributions from 86 countries, the programme committees of the 7 conferences have carefully selected 350 papers, which are presented at the conference and printed in this proceeding

The conferences which you are allowed to switch from one to another cover the main technical aspects of the global information society, like basic theories in the Fundamentals and IT & Knows conference, the hot topics security and legal conditions using net and computers, and important applications such as teleteaching, telecooperation and the use of computers by people with special needs. In the keynote sessions, outstanding experts will introduce the fundamental technologies which made and will continue to make information society possible.

The congress is accompanied by a set of panels, tutorials and workshops. I would like to draw your special attention to the Youth Summit. It will be for the first time

that young people will have the opportunity to articulate their views and expectations to the IT community and politicians.

The programme gives a good opportunity to study the major technologies and applications which will be the base of future society and to discuss its impact with colleagues from more than 80 countries of our globe.

I hope you enjoy the programme, which was so carefully assembled by about 200 ladies and gentlemen in the various programme committees, and that your attendance at the congress will have a positive impact on your professional work.

Furthermore, I am sure, that this proceeding will gain a good position in your personal technical library.

Egon Hörbst
Siemens AG Munich,
Technical University of Munich,
International Programme Committee Chair

Introduction by the Programme Committee IFIP SEC '98

The annual conference of Technical Committee 11, SEC '98, covers a wide range of security related topics. The conference concentrates on technical as well as on commercial aspects of information security. With the emerging importance of modern communication technologies, as well as the growth of the global electronic marketplace, SEC '98 places a special focus on the information security aspects of electronic commerce in the Global Information Infrastructure.

With its series of SEC conferences, TC11, under the auspices of IFIP, is actively contributing to both technical and societal aspects of information security. For the first time the SEC conference is a part of the IFIP World Computer Congress. As such, this is an opportunity to effectively and formally express the fact that information security is an integral part of the wider IT environment.

SEC '98 is an event which wants to make the statement that security technology is on its way from being an add on technology to become a basic infrastructure.

With the WCC '98/SEC '98 conferences, IFIP/TC11 is responding to rapidly developing standards in the IT field, as well as their human impact. Besides presenting a forum for information exchange in the technical, management, and societal arena, IFIP is emphasising opportunities in areas like education of an increasingly broad public, generating user awareness, ongoing policy monitoring, legal issues and others in the wider IT field.

By being part of the WCC '98, this SEC '98 conference shows that IT-Security is an enabling technology of today and tomorrow.

The Programme Committee IFIP SEC '98

IFIP SEC '98 Conference Committees

Joint Conference chair

György Papp, Prime Minister's office, Hungary
Reinhard Posch, Graz University of Technology, Austria

Programme Committee

David Batchelor, Sussex Systems Ltd., Canada
William J. Caelli, Queensland University of Technology, Australia
Jan Carlsen, Coopers & Lybrand, Denmark
Dimitris Gritzalis, Athens University of Economics & Business, Greece
Patrick Horster, University of Klagenfurt, Germany
Sokratis Katsikas, University of the Aegean, Greece
William List, The Kingswell Partnership, United Kingdom
Tibor Nemetz, HunGuard Ltd., Hungary
Jean-Jacques Quisquater, University of Louvain, Belgium
Pierangela Samarati, SRI International, Italy
Sebastian von Solms, Rand Afrikaans University, South Africa
Willis Ware, The Rand Corporation, USA
Tibor Vámos, Hungary
Louise Yngström, University of Stockholm, Sweden

Referees

Mads Bryde Andersen, University of Piraeus, Greece
Richard Baskerville, Georgia State University, USA
Vesselin Bonchev, FRISK Software Int., Iceland
Klaus Brunnstein, Hamburg University, Germany
Michael Burmester, University of London, United Kingdom
William J. Caelli, Queensland University of Technology, Australia
Jan Carlsen, Coopers & Lybrand, Denmark
V. Chrissikopoulos, University of Piraeus, Greece
Ed Dawson, Queensland University of Technology, Australia
Lynette Drevin, Potchefsstroom University, South Africa
Jan Eloff, Rand Afrikaans University, South Africa
Viiveke Fåk, Linköping University, Sweden
Simone Fischer-Hübner, University of Hamburg, Germany
Sara Gordon, Command Software Systems, USA
Dimitris Gritzalis, Athens University of Economics & Business, Greece
Patrick Horster, University of Klagenfurt, Germany
Sushil Jajodia, George Mason University, USA
Erland Jonsson, Chalmers University of Technology, Sweden
Jorma Kajava, University of Oulu, Finland

Referees (cont'd)

Sokratis Katsikas, University of Aegean, Greece
Klaus Keus, German Information Security Agency, Germany
E. Kiountouzis, Athens University of Economics & Business, Greece
Svein Johan Knapskog, University of Trondheim, Norway
Peter Lipp, Graz University of Technology, Austria
William List, The Kingswell Partnership, United Kingdom
Juha E. Miettinen, Telecom, Finland
Sead Muftic, Stockholm University, Sweden
György Papp, Prime Minister's office, Hungary
Heike Paschinger, Academy of Sciences, Austria
Günter Pernul, University of Essen, Germany
Hartmut Pohl, Germany
Karl Posch, Graz University of Technology, Austria
Kai Rannenberg, University of Freiburg, Germany
Christian Reiser, Eunet, Austria
Pierangela Samarati, SRI International, Italy
Ingrid Schaumüller, Austria
Leon Strous, De Nederlandsche Bank, The Netherlands
Sebastian von Solms, Rand Afrikaans University, South Africa
Willis Ware, The Rand Corporation, USA
Petra Wohlmacher, University of Klagenfurt, Austria
Louise Yngström, University of Stockholm, Sweden

Student Paper Award Committee

Reinhard Posch, Graz University of Technology, Austria (Chair)
Louise Yngström, Stockholm University, Sweden

Kristian Beckman Award Committee

Reinhard Posch, Graz University of Technology, Austria
Sebastian von Solms, Rand Afrikaans University, South Africa
Louise Yngström, University of Stockholm, Sweden

Organising Committee

Co-Chairs: Dr. Walter Grafendorfer, Mrs. Maria Tóth
Austrian members: Wolfgang Hawlik, Daniela Pötzl, Klaus Sarg, Wolfgang Resch
(Austrian Computer Society)
Hungarian members: Csilla Bánfi, Gizella Hetthessy, Emese Kövér,
Eszter Zubovics (John von Neumann Computer Society)

INDEX OF CONTRIBUTORS

Aedo, I. 251
Apostolopoulos, T.K. 567
Aslan, H. K. 173

Baranyi, L. 491
Baskerville, R. 549
Bauknecht, K. 477
Bekmann, J. P. 333
Bognár, G. 601
Bonifácio Jr, J. M. 418
Borrell, J. 206
Brehel, J. 607
Bruschi, D. 449
Burge, M. 139
Burger, W. 139
Buttyán, L. 111

Cahn, R. 123
Cansian, A. M. 418
Carvalho, A. C. 418
Chang, H. 504

Dacier, M. 405
Dawson, S. 285
de Goede, P. 333
Debar, H. 405
Deswarte, Y. 321
Díaz, P. 251
Dittmann, J. 24
Dusollier, S. 344

Eckert, C. 184
El-Hadidi, M. T. 173
Eloff, J.H.P. 592

Franz, E. 554

Gamage, C. 575
Garay, J. A. 123
Gast, T. 467
Gorrieri, R. 15
Graubner, A. 554
Gregory, D. 586
Gritzalis, S. 3
Großschädl, J. 515

Hartmann, A. 484
He, O. 196
Hegazi, N. H. 173
Heikkuri, S. 271
Hickson, N. 441
Higaki, H. 230
Holbein, R. 160
Hornák, Z. 611
Horster, P. 37
Hutchison, A. C. M. 333

Iliadis, J. 3
Imai, H. 75, 96
Iyengar, A. 123

Janczewski, L. J. 149
Jazayeri, M. 535
Jerichow, A. 554
Jerman-Blazic, B. 509
Jøsang, A. 541
Jutla, C. 123

Kabasele-Tenday, J.-M. 580
Kajava. J. 309
Keus, K. J. 467
Kincses, Z. 611
Kirsch, P. 477
Klobucar, T. 509
Knapskog, S. J. 541
Kozik, E. 561
Kuch, R. 49

Lam, K. Y. 297
Laurent, M. 523
Leiwo, J. 271, 575
Lioy, A. 61
Lipp, P. 49
Lo, B. K. W. 149
Louwrens, C. P. 240

Maino, F. 61
Marchetti, G. 15
Mayerwieser, W. 355
Merabti, M. 586
Michaljević, M. 96
Mohay, G. 530
Moreira, E. S. 418
Morger, O. 160
Moulinos, K.D. 567

Nemetz, T. 366
Nitsche, U. 160

Oikonomou, V. 3
Okamoto, E. 297
Olejar, D. 499
Ortalo, R. 321

Pancho, S. 455
Papp, G. 601
Papp, P. 366
Pfitzmann, A. 554
Posch, K. C. 355
Posch, R. 355
Prentner, W. H. 535
Pries-Heje, J. 549

Qian, S. 285

Ribagorda, A. 251
Riera, A. 206
Rifà, J. 206
Rosti, E. 449

Samarati, P. 285
Schartner, P. 37
Schier, K. 219
Shi, Q. 586
Singhal, M. 460
Siponen, M. T. 309
Smith, E. 592
Spruit, M. E. M. 392
Staamann, S. 111
Stabenau, M. 24
Stanek, M. 499
Steinmetz, R. 24
Sterbenz, A. 49
Su, Z. 196
Subramanian, S. 460
Szabó, I. 601

Takizawa, M. 230
Teufel, S. 160
Trommler, P. 261

von Solms, S. H. 240

Wang, X. F. 297
Warren, M. J. 429
Weidner, H. 477
Wespi, A. 405
Wilhelm, U. 111
Wohlmacher, P. 37

Yasuda, M. 230
Yi, X. 297
Yngström, L. 381

Zhang, C. N. 85
Zheng, Y. 75, 96, 575

KEYWORD INDEX

access control 160, 230, 580
algorithm approach 85
anomaly detection 405
anonymity 554
anti-virus technology 240
application profiles 261
assurance 541
asymmetric crypto. Algorithm 467
ATM 535
attacking model 554
audit 607
authentication 173, 586
automatic verification 184
autonomous agent 586, 240

biological model 240
blind signature 196
business processes 160

cellular automata 96
certificate policy 509
certification authority 49, 467
China's INTERNET security 561
COBRA 111
comparison 509
comprehensive IT-security 484
computer security 240, 405, 549
confidentiality 554
context-dependency 160
controls 607
coprocessor 355
copyright protection 24
countermeasures 392
cross-cultural study 381
cryptographic primitives 96
cryptographic protocol 184
cryptography 355, 491
Cyber terrorism 429

data integrity 96
data security 366
database security 285
DES 355
design 607
design and analysis tools 333
design model 251
digital cash 449
digital signature 49, 75, 85, 366, 467, 504
distributed patient records 592
distributed storage 123
distributed systems 285
downloaded executable content 261
DPE 111

ear biometrics 139
e-commerce 24, 219, 309, 449, 460, 477
electronic certification 366
electronic payment systems 219
electronic voting 196
electronic voting schemes 206
electronic/Internet banking 607
elliptic curves 75
Encryption 75
encryption/decryption 504
ERMS 344
error detection 85, 366
ethics and information security 271
evaluation 499

fault tolerance 85
firewalls 561
formalisation 509
fuzzy logic 592

generalized Voronoi diagrams 139
global Information Infrastructure 455

health care 592
hospital information systems 149
human behaviour 392
human failure 392
hypermedia 149, 251

immune system 240
implementation 160
information dispersal 123
information flow control 230
information security 123, 149, 575,
information security policy 607
information systems 321
information technology controls 549
information transmission security 366
Internet 219, 429, 455, 477
interoperability 111, 285
Intrusion detection 405, 418, 586
IPR Management 344
IT- Security 607
IT security awareness 381

Java 261

KerberosV5 535
key distribution 173
key generation 37
key management 37
key randomness 37
Key recovery 491

key uniqueness 37

legal 344
logic analysis 173
logic of authentication 184
Lotus Notes 491

macro cell 355
management information base 567
mix model 554
mobile agent 586
modeling 355
modular multiplication 515
multifunctional smartcards 219
multilevel security 285
multiple certification authorities 504

network and web security 61
network design 561
network management 567
network security 418, 523
neural networks 418

obbac model 580
object oriented modelling 575
object-based systems 230
one-way hash functions 96
OSF/DCE 535

passive identification 139
payment protocol 449
PGP 491
pipelined multiplier 515
planning 607
prevention 392
privacy 554
privilege graph 321
program integrity 530
protocol engineering 333
public encryption 173
public key certificates 61, 75, 85, 504, 509
public key cryptography 75, 85
public key infrastructure 504, 509
public sector 49
purpose-oriented model 230

quantitative evaluation of security 321

randomness 366
real-time 460
reference monitor 149
responsibility 484
risk 429, 592
role and task based security model 219
role based access control 61
RPC 535
RSA 85, 355, 515

Safeguards 549
secure code distribution 530
secure interconnection systems 271
security 111, 219, 251, 392, 530, 554, 580, 586
  and the media 24
  conception 477
  context 111
  domain 567
  evaluation 541
  management 271, 541
  model 261, 580
  policy 467, 567
  protocols 333
  services 523
  technology 561
  threats 309
SesameV4 535
signcryption 75
smartcards 206
SNMP 567
social questions 484
software Metrics: LOC, FPA 535
SSLeay 535
strategic management 607
subjective logic 541
symmetric cryptosystem 499
symmetric encryption 173

TCP/IP 535
technology assessment 484
tests for randomness 366
threats 592
threshold cryptography 123
time stamp 366
TINA 111
TQM, TR/SM 607
trust 541

uncoercibility 206

VLSI design 355, 515
vulnerabilities 592

watermarking for MPEG video 24
WWW 449

X.509 49, 504

ACKNOWLEGDEMENTS

MAIN SPONSORS OF THE XV. IFIP WORLD COMPUTER CONGRESS 1998

as of 18 July 1998, in alphabetical order

Austrian Federal Ministry of Science and Transport

City of Vienna

European Union

Foundation for Technological Development of Industry

Hungarian Government

IBM Austria, IBM Hungary

ORACLE Austria, ORACLE Hungary

Sun Microsystems

Vienna Tourist Board

SPONSORS

Austrian Federal Ministry for Education and Cultural Affairs; Hungarian Telecom; Hungarian Tourist Board; MATÁV, Hungary; National Committee for Technological Development, Hungary; Post & Telekom Austria; Public Foundation for Open Vocational Training, Hungary; SAP Austria; Siemens Austria; SONY DADC Austria; Taverna, Hungary

COOPERATING ORGANIZATIONS

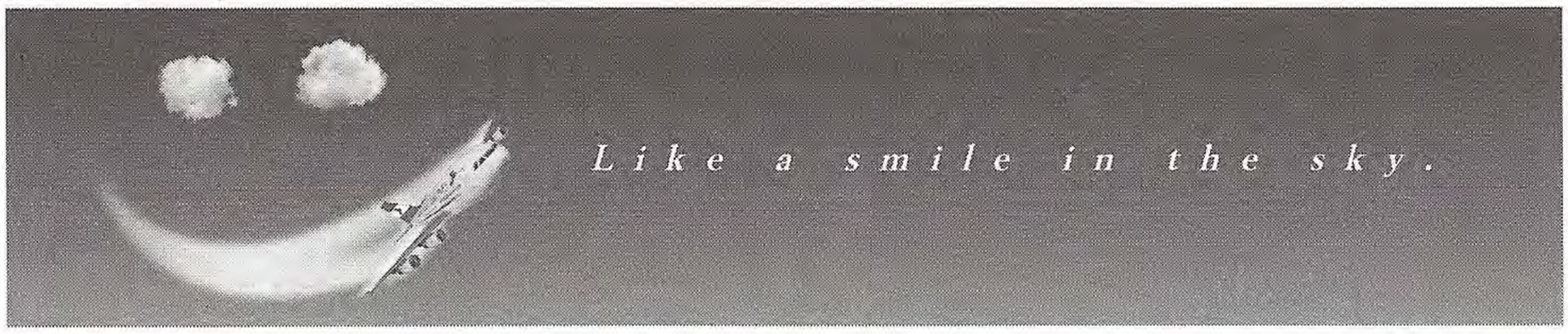
CEPIS; European Oracle User Group (EOUG); Forum Info2000; Vienna University of Technology

Special thanks to all IFIP and CEPIS member societies that supported the organizers in preparing this event.

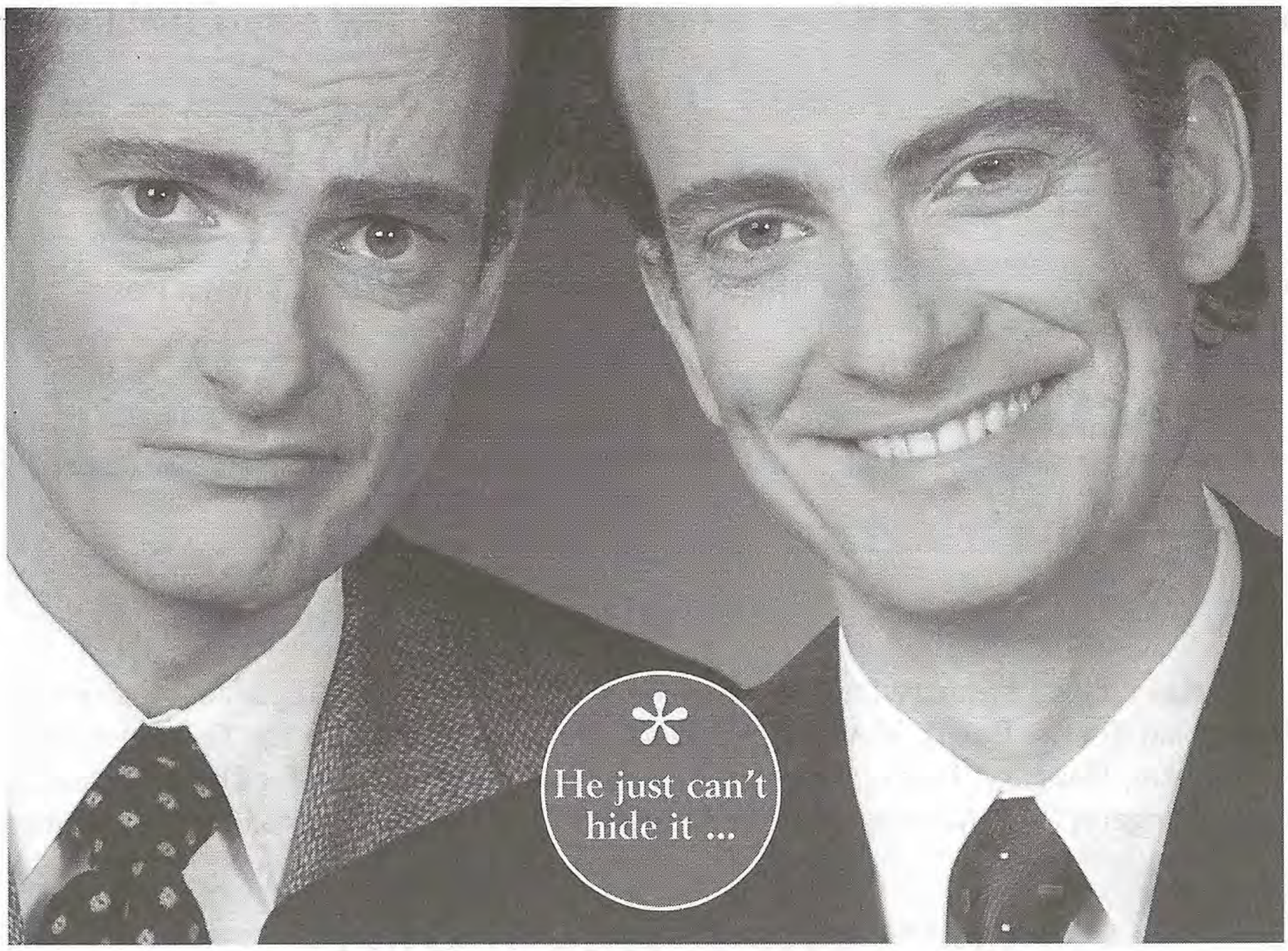
OFFICIAL CARRIER

AUA - Austrian Airlines

MALEV, Hungarian Airlines



GUESS which of these two men flies with *Austrian Airlines.**



Some things in life are so simple. A smile for example. It says everything about a person. Or about an airline.

So we have no excuse. If we want to find out if you're happy travelling with us we just have to look at you.

It will be written all over your face.

Visit our most friendly website: http://www.aua.com

AUSTRIAN AIRLINES

THE MOST FRIENDLY AIRLINE.

GRILL + GULL · THOMPSON

INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING (IFIP)

IFIP was founded in 1960 under the auspices of UNESCO. Its basic aims are to promote information in science and technology by fostering international cooperation, by stimulating research, development and the applications of information processing in science and human activity, by furthering the dissemination and exchange of information and by encouraging education in information processing. IFIP is a multinational federation of professional and technical organizations concerned with information processing. Currently it has 44 Full National Members, 3 Corresponding Members, 1 Associate Member and 11 Affiliated International Organizations representing all regions of the World.

IFIP's flagship event is the World Computer Congress, currently held biannually. In addition there are major international conferences and other events organized by IFIP's Technical Committees. Annually, IFIP is involved in the organization of over 65 events leading to some 30 to 40 IFIP books.

Preparations are under way for the 16th IFIP World Computer Congress, which will be held from 21 to 25 August 2000 in Beijing, China.

The core of IFIP's scientific work is carried-out by its 12 Technical Committees (with over 70 working groups):

TC 1 FOUNDATIONS OF COMPUTER SCIENCE

- WG 1.1 Continuous Algorithms and Complexity
- WG 1.2 Descriptional Complexity
- WG 1.3 Foundations of Systems Specifications
- WG 1.4 Computational Learning Theory
- WG 1.5 Cellular Automata and Machines

TC 2 SOFTWARE THEORY AND PRACTICE

- WG 2.1 Algorithmic Languages and Calculi
- WG 2.2 Formal Description of Programming Concepts
- WG 2.3 Programming Methodology
- WG 2.4 System Implementation Languages
- WG 2.5 Numerical Software
- WG 2.6 Database
- WG 2.7 User Interface Engineering (WG 13.4)
- WG 2.8 Functional Programming
- WG 2.9 Software Requirements Engineering

TC 3 EDUCATION

- WG 3.1 Informatics Education at the Secondary Education Level
- WG 3.2 Informatics Education at the University Level
- WG 3.3 Research on Education Applications of Information Technologies
- WG 3.4 IT Professional and Vocational Education in Information Technology
- WG 3.5 Informatics in Elementary Education
- WG 3.6 Distance Learning
- WG 3.7 Information Technology in Education Management

TC 5 COMPUTER APPLICATIONS IN TECHNOLOGY

- WG 5.2 Computer-Aided Design
- WG 5.3 Computer-Aided Manufacturing
- WG 5.4 Industrial Software Quality and Certification
- WG 5.6 Maritime Industries
- WG 5.7 Integrated Production Management
- WG 5.10 Computer Graphics & Virtual Worlds
- WG 5.11 Computers and Environment
- WG 5.12 Architectures for Enterprise Integration

TC 6 COMMUNICATION SYSTEMS

- WG 6.1 Architecture and Protocols for Computer Networks
- WG 6.2 Broadband Communications
- WG 6.3 Performance of Communication Systems
- WG 6.4 High Performance Networks
- WG 6.6 Network Management for Communication Networks
- WG 6.7 Intelligent Networks
- WG 6.8 Wireless Communications
- WG 6.10 Photonic Communication Networks

TC 7 SYSTEM MODELLING AND OPTIMIZATION

- WG 7.1 Modelling and Simulation
- WG 7.2 Computational Techniques in Distributed Systems
- WG 7.3 Computer Systems Modelling
- WG 7.4 Discrete Optimization
- WG 7.5 Reliability and Optimization of Structural Systems
- WG 7.6 Optimization-Based Computer-Aided Modelling and Design
- WG 7.7 Stochastic Optimization

TC 8 INFORMATION SYSTEMS

- WG 8.1 Design and Evaluation of Information System
- WG 8.2 The Interaction of Information Systems and the Organization
- WG 8.3 Decision Support Systems
- WG 8.4 Office Information Systems
- WG 8.5 Information Systems in Public Administration
- WG 8.6 Transfer and Diffusion of Information Technology
- WG 8.7 Informatics in International Business Enterprises

TC 9 RELATIONSHIP BETWEEN COMPUTERS AND SOCIETY

- WG 9.1 Computers and Work
- WG 9.2 Social Accountability
- WG 9.3 Home Oriented Informatics and Telematics
- WG 9.4 Social Implications of Computers in Developing Countries
- WG 9.5 Applications and Social Implications of Virtual Worlds
- WG 9.6 Information Technology Misuse and the Law
- WG 9.7 History of Computing

TC10 COMPUTER SYSTEMS TECHNOLOGY

- WG 10.1 Computer-Aided Systems Theory
- WG 10.3 Concurrent Systems
- WG 10.4 Dependable Computing and Fault Tolerance
- WG 10.5 Design and Engineering of Electronic Systems
- WG 10.6 Neural Computer Systems
- WG 10.7 Microsystems

TC 11 SECURITY AND PROTECTION IN INFORMATION PROCESSING SYSTEMS

- WG 11.1 Information Security Management
- WG 11.2 Small System Security
- WG 11.3 Database Security
- WG 11.4 Network Security
- WG 11.5 Systems Integrity and Control
- WG 11.8 Information Security Education

TC12 ARTIFICIAL INTELLIGENCE

- WG 12.2 Machine Learning
- WG 12.5 Knowledge-Oriented Development of Applications

TC13 HUMAN-COMPUTER INTERACTION

- WG 13.1 Education in HCI and HCI Curricula
- WG 13.2 Methodology for User-Centered System Design
- WG 13.3 Human-Computer Interaction and People with Special Needs

For further detailed information on IFIP and its activities please visit the IFIP Web site at http://www.ifip.or.at

or contact the IFIP Secretariat:
Hofstrasse 3, A-2361 Laxenburg, Austria
Tel. +43 2236 73616,
Fax: +43 2236 73616 9,
e-mail: ifip@ifip.or.at